



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/622,338	07/18/2003	Wolfgang S. Hammersmith	44461660-7031	4844

26263 7590 11/17/2006

SONNENSCHN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER

DINH, MINH

ART UNIT PAPER NUMBER

2132

DATE MAILED: 11/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/622,338	HAMMERSMITH ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☐ Claim(s) 1-9, 11-20 and 22-25 is/are rejected.
- 7) ☒ Claim(s) 10 and 21 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 July 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. ____. |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>12/16/03, 1/20/04.</u> | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-25 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: (i) compressing the transport key to form a compress transport key (see figure 1, step 6; Specification, page 14, lines 10-16), and (ii) using one-time pad scheme for the encrypting and decrypting steps (Specification, page 16, lines 9-15, 21-24).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United

States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-5, 12-20, 22-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Howard, JR. et al. (US 2001/0026619) (hereinafter "Howard"). Howard discloses a method and apparatus for managing key material (e.g. distributing certificates and keys) in cryptographic devices using a integrated key management system (IKMS) (Abstract; figure 3).

Regarding claims 1-5, 12-15 and 24-25, Howard specifically discloses a method for the IKMS to securely distribute a unique device private key to a cryptographic device in the Device Initialization phase, said method comprising the steps of: combining the cryptographic key (i.e., encrypted private key) with a transport key (i.e., the KEA public values used by the cryptographic device later to decrypt the encrypted private key) to form a key set (i.e., an envelope); encrypting the key set to form an encrypted key set (i.e., an encrypted envelop); distributing the encrypted key set across a medium; and decrypting the encrypted key set to reconstitute the transport key and the cryptographic key (paragraphs 0057, 0211-0216).

Regarding claims 16-19, Howard further discloses that, upon completion of the Device Initialization phase, the IKMS uses the same method to securely distribute other keys in the next phase, the Secure Key

Transport phase (paragraphs 0217-0222). Howard also discloses that distribution of a new key is automatically performed when a current cryptographic key is about to expire (paragraphs 0086, 0161).

Regarding claims 20 and 22-23, Howard further discloses that the encrypting step is performed by a Diffie-Hellman session KEK (key encryption key) comprising the transport key and a conversion key (paragraph 0067).

6. Claims 1-5, 12-14, 16 and 24-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Ishiguro et al. (US 2006/0159272). Ishiguro discloses a method and system for updating cryptographic keys using a tree structure and an enabling key block EKB comprising a set of keys (Abstract; figures 3, 4A-B; paragraphs 0108-0115). Specifically, Ishiguro discloses a method for securely distributing a cryptographic key (i.e., content key Kcon for decrypting encrypted content), said method comprising the steps of: combining the cryptographic key (i.e., encrypted Kcon) with a transport key (i.e., the enabling key block EKB used to decrypt the encrypted Kcon) to form a key set (a key message); encrypting the key set using the session key Kses to form an encrypted key set (i.e., an encrypted key message); distributing the encrypted key set across a medium; and decrypting the

encrypted key set to reconstitute the transport key and the cryptographic key (figure 16, paragraphs 0166-0168).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 6-8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro as applied to claim 1 above, and further in view of Benaloh (6,886,098). Ishiguro discloses that the transport key comprises a set of keys. Ishiguro does not disclose compressing the transport key. Benaloh discloses compressing a set of keys (figure 14, element 1432; col. 1, lines 12-16, 36-39, 66-67; col. 2, lines 1-5; col. 15, lines 44-59). It would have been obvious to one of ordinary in the art at the time the invention was made to modify Ishiguro method to compress the set of keys which constitutes the transport key, as taught by Benaloh. The motivation for doing so would have been to reduce the data volume to be transmitted.

9. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro and Benaloh as applied to claim 6 above, and further in view of Fish (6,411,227). Ishiguro and Benaloh do not disclose that the compressing step is performed using sliding window compression. Fish discloses compressing data using sliding window compression, which is a lossless compression technique (col. 1, line 62 – col. 2, line 25). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the combined method of Ishiguro and Benaloh to use sliding window compression, as taught by Fish. The motivation for doing so would have been to avoid data loss during the process of compressing and depressing data.

Allowable Subject Matter

10. Claims 10 and 21 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Double Patenting

11. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by

multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

12. Claims 1-25 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-20 of copending Application No. 2004/0136537. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of the copending Application contain(s) every element of claims 1-25 of the instant application and as such anticipate(s) claims 1-25 of the instant application.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

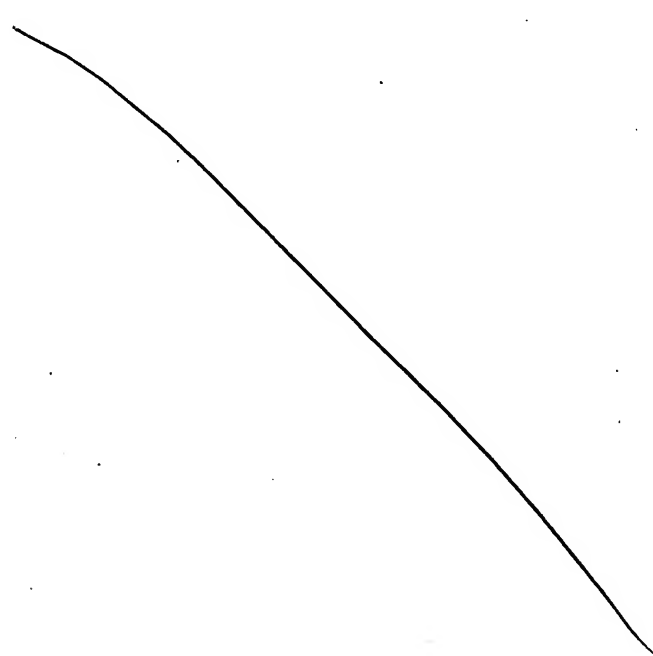
Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,862,582 to Harada et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

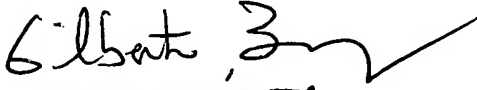


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

MD
11/12/06


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100